

SEL Secure Solutions



SEL experts and solutions help you secure critical infrastructure

- Create a baseline of your current operational technology (OT) system, and identify potential vulnerabilities.
- Address gaps with secure network solutions, and achieve standards compliance with minimal disruption to operations.
- Streamline compliance efforts with centralized asset management, software and firmware updates, event logs, and password rotations.
- Detect cyber events, and ensure an effective response and prompt system restoration.



Consider these questions to identify cybersecurity gaps

RESOURCES

How is your cybersecurity team structured?

IT and OT systems have different performance requirements. We can help you implement cybersecurity strategies that minimize disruption to OT environments.

Who manages your OT communications systems?

Day-to-day operations require specialized skills. We offer knowledgeable staff and resources to assist you with each aspect of OT system ownership.

Who monitors the security of your system?

Proper design of event notification systems is crucial to situational awareness. We help design and implement turnkey security monitoring solutions, and we offer 24/7/365 monitoring services via our Security Operations Center.

FRAMEWORK

Do you have an OT cybersecurity framework?

SEL secure solutions are designed around the National Institute of Standards and Technology (NIST) cybersecurity framework, which enables compliance with other security frameworks, such as NERC CIP and IEC 62351. We can help develop a road map for implementing these solutions and can provide constant system monitoring.

Are you required to comply with cybersecurity standards?

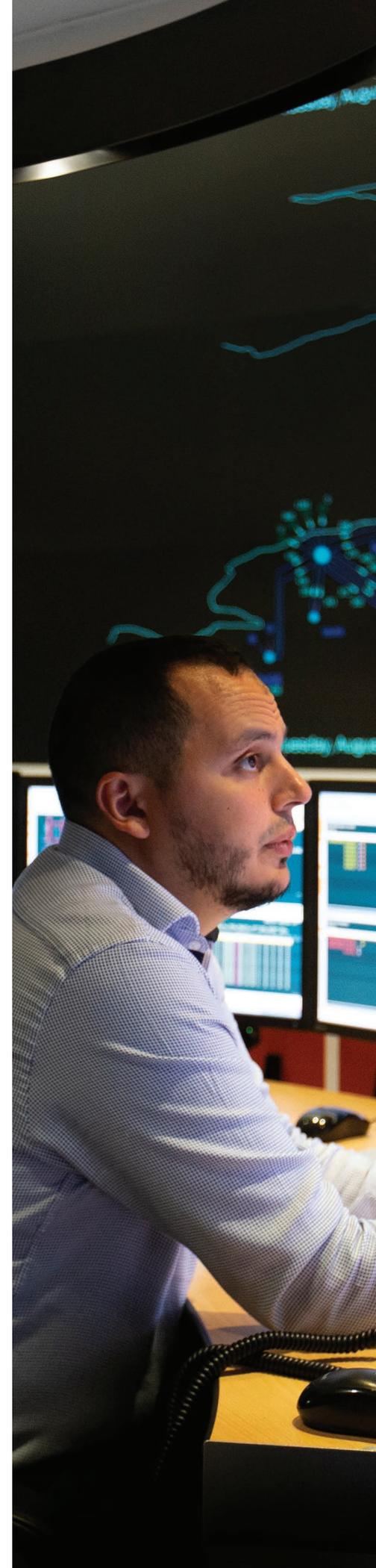
We offer assessment services that confirm compliance with cybersecurity standards, and we can provide hardening guides for computers, relays, and controllers.

Is physical security integrated into your cybersecurity framework?

Physical security is part of the defense-in-depth approach to cybersecurity. SEL solutions take into account physical security, along with natural and environmental disasters, to provide a holistic view of cybersecurity risks.

Is vendor supply chain security one of your current considerations?

At SEL, we understand the importance of securing our supply chain and follow rigorous internal and external processes to qualify our products and applications. We own every line of our software and firmware code. This code is digitally signed, never shared outside of SEL, and continuously monitored for new threats. When you choose an SEL solution, you can be sure it is secure.





NETWORK DESIGN

When was the last time you had a third-party network audit performed?

We offer onsite assessment and compliance audits to support your needs.

How do you secure network links for remote access?

We provide network design, consulting, and implementation of secure, encrypted remote access solutions.

Have your OT devices been hardened?

We offer networking solutions that use software-defined networking (SDN) to whitelist approved network flows, disable unused ports and services, and eliminate several attack vectors of traditional LANs.

PROCESSES TO MAINTAIN SECURITY

What is the process for asset management on your OT systems?

Asset management for large systems can be a challenging task. SEL asset management software can help reduce the cost of operations and simplify patch management update processes.

How are user accounts managed for your OT devices?

OT networks have many devices with several permission levels. Passwords must be securely rotated and user permissions assigned appropriately. We offer centralized user account management to simplify operations and user account maintenance.

How do you manage version control of system settings?

Creating and maintaining a baseline of system settings is a crucial component of system ownership. We can provide asset management software that simplifies system baselining and version control.

How do you approach patch management?

Understanding which patches are applicable and how to securely deploy updates can be challenging. We offer patch management services that monitor vulnerability notices, and we deliver a tested mitigation plan.

DETECTION AND RESPONSE

Are you prepared to detect cyber events on your system?

There are many indicators of compromise that point to potentially malicious activity and known tactics that attackers use. SEL secure solutions detect intrusions, and we provide playbooks for response procedures.

Do you review recovery processes via tabletop exercises?

Policies and procedures are most beneficial when personnel are properly trained. We offer tabletop exercises to test personnel knowledge and the effectiveness of response procedures. Services like automatic settings backup can aid in the recovery process.

Why SEL?

With extensive OT and cybersecurity expertise, we build effective turnkey solutions that improve cybersecurity and streamline asset management and ongoing compliance. An SEL secure solution will be ready to defend against and prevent vulnerabilities and will not negatively impact other OT system requirements. SEL offers a broad portfolio of solutions and experts to do the work, as needed.

Next steps

Contact SEL at secure@selinc.com to connect with our team of OT cybersecurity experts.



SEL Engineering Services
+1.509.332.1890 | secure@selinc.com | selinc.com

© 2019 by Schweitzer Engineering Laboratories, Inc.
LM00413-01 • 20191003